Profiles

MACTECH

Kirk Godtfredsen

Kirk has over 24 years of Mac related IT experience - from StarControllers and 3270 emulation over Token Ring to WPA, Active Directory and iPhones, he's had to integrate it.

He spent 13 years at Apple as a systems engineer and trainer (before the stock splits - natch). For the last 11 years he has provided IT support to small biz, K-12 and higher-education, and also spends time helping out @ BusyMac, the makers of BusyCal.

He has been involved with mobile computing since its inception, working on the first email client for the first internet-based phone w/AT&T Wireless. When he isn't working, he's biking and hiking.

MACTECH

Agenda

- Profiles explained
- Delivering Profiles and the MDM
- New Application Management in iOS7/ MacOSX10.9
- Some fun w/Configurator and Meraki
- QandA

What are Profiles?

- Profiles contain settings and preference bundles for devices including:
  - Restrictions on device features
  - Wi-Fi settings
  - VPN settings
  - Email server settings
  - Exchange settings
  - LDAP directory service settings
  - CalDAV calendar service settings
  - Wallpaper
  - Web clips
  - Credentials and keys

MACTECH

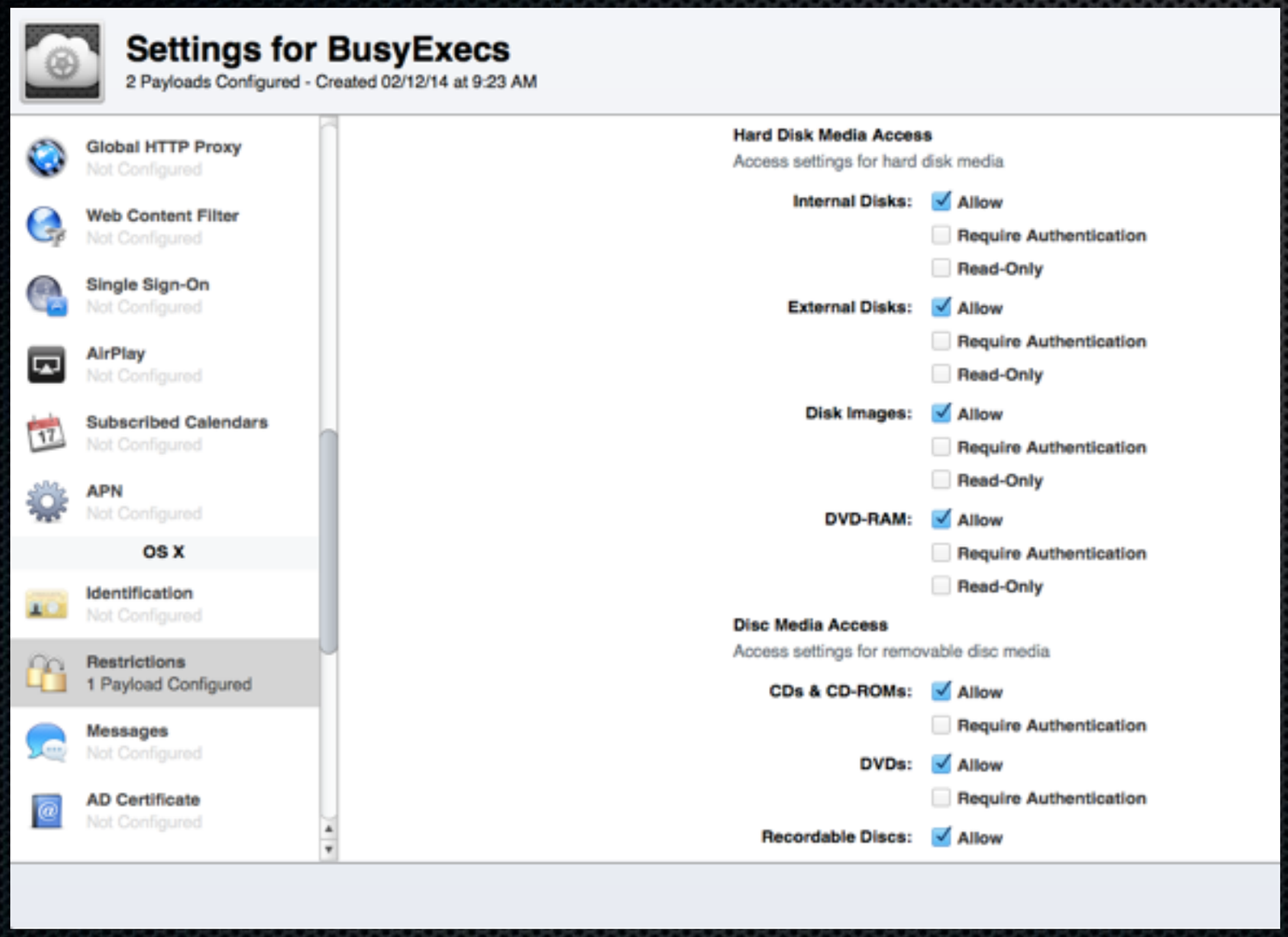
Profile Basics

- Why use them?
- Signed vs. Unsigned Profiles
- Profiles can be user/group or device centric
- Profile Delivery
  - Apple Configurator
  - MobileDeviceManagement (MDM)
  - or email/web, USB stick/etc (it's just a file…)

Terms and things you need to know:

- .mobileconfig
  - xml files that store profile info
  - based on OS X preference file format
  - profiles are made up of payloads
- Trust profile
  - needed for self-signed servers
- Enrollment profile
  - provided by MDM for enrollment
  - binds the device to the MDM

Profile.mobileconfig…




```
<key>PayloadDisplayName</key>
<string>Restrictions</string>
<key>logout-eject</key>
<dict/>
<key>mount-controls</key>
<dict>
  <key>blankcd</key>
  <array/>
  <key>blankdvd</key>
  <array/>
  <key>cd</key>
  <array/>
  <key>dvd</key>
  <array/>
  <key>dvdram</key>
  <array/>
  <key>disk-image</key>
  <array/>
  <key>harddisk-external</key>
  <array/>
  <key>harddisk-internal</key>
  <array/>
 </dict>
</dict>
<dict>
  <key>PayloadType</key>
  <string>com.apple.DiscRecording</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>PayloadIdentifier</key>
  <string>com.apple.mdm.ml.kkheconsulting.com.8aca65e0-7032-013
  <key>PayloadEnabled</key>
  <true/>
  <key>PayloadUUID</key>
  <string>60c20226-fa71-aafc-8332-1302aa02d6bc</string>
  <key>PayloadDisplayName</key>
  <string>Media Access:  Disc Recording</string>
  <key>BurnSupport</key>
  <string>on</string>
</dict>
<dict>
```

MACTECH

Why Apple Configurator (still)

- No way to "Supervise" a device over the air
  - Certain attributes can only be managed if device is supervised (Airdrop)
- No way to lock an over the air MDM enrollment profile so user can't remove it
- No way to distribute and then revoke apps using just one Apple ID.
- Great way to generate Profiles for use in other tools…

APNS

Apple Push Notification Service

MACTECH

APNS

Apple
17.0.0.0/8

Persistent Connection

port 5223/alt 443

Devices

Port 80/443/8443 (depending on MDM)

port 1640 Enrollment

port 2196

port 2195

MDM

MACTECH

Firewalls

- For APNs traffic to get past your firewall, you'll need to open these ports:
  - TCP port 1640 for enrollment (Apple PM)
  - TCP port 5223 (used by devices to communicate to the APNs Servers)
  - TCP port 2195 (used to send notifications to the APNs)
  - TCP port 2196 (used by the APNs feedback service)
  - TCP port 443 (used as a fallback on Wi-Fi only, when devices are unable to

APNs: Load Balancing

- Apple Push Notification Service (APNs) servers use load balancing.
- Your devices will not always connect to the same public IP address for notification.
- The entire 17.0.0.0/8 address block is assigned to Apple, so it's best to allow this range in your firewall settings.

MDM

- Creating an enrollment profile (and trust if self-signed)
- Creating and installing configuration profiles
  - Apply payloads effectively
  - Payload interactions
  - Payload variables
- User/Group/Device management
- Managing in-house enterprise apps for users and user groups
- Best reference - OS X Server help:
  - https://help.apple.com/profilemanager/mac/3.0/#apdE3493-C50A-4E9E-A1B6-CBCBC8C73507

MACTECH

Managed Distribution of Apps and Books

- Although coupled with MDM, independent service
- Linked to Apple's Volume Purchase Program (VPP) for Ed and Biz
- Old model - iTunes Store codes. You buy/user owns
- Managed Distribution - You buy, you give via App Store, you revoke, they buy if they want
- Big key - everyone has an Apple ID
- Works for both Mac and iOS Apps

Compare and Contrast leading MDM solutions

- Countless players
- Compare and contrast
- Find the features you need
- Great resource at:
  http://www.enterpriseios.com/wiki/Comparison_MDM_Providers

MACTECH

Main Uses and Differences

- What features should you be looking for?
- What size solution do you need?
- Who will maintain it?
- Where do they excel?
- How do you choose?

MACTECH

Main Players

- Absolute
- Apple Profile Manager
- BoxTone
- Centrify
- Filewave
- JAMF Casper Suite
- MaaS360 by Fiberlink
- Meraki
- MobileIron
- SOTI

In action - Olympics:

Apple Configurator

Meraki Dashboard

Apple VPP

MACTECH

Sochi iPad

- 1000 iPads for use within Olympic Village
- Check in/Check out (recharge each eve, when power works!)
  - Country fined 1,000 rubles for non-return
- Olympic Private WiFi
- Browser/Custom Olympic Apps for housing/maps/etc
  - lots of data, not updated much
- Sounds like a Job for Apple Configurator!

MACTECH

Sochi BYOD

- Access to Olympic wifi (not public)
- Web clips for Olympic Athlete Intranet
  - Once enrolled and register Apple ID on intranet
    - Promote use of Spark for “on the ground” athlete created videos
- Sounds like a job for Meraki and Apple VPP

Questions?

Kirk Godtfredsen
kirkg@kkheconsulting.com

MACTECH